CLAIMS

What is claimed is:

1.   A computing system comprising:

at least one random access memory (RAM), the RAM having a storage location containing filesystem data with associated page table entries, each page table entry having a read/write flag for the filesystem data, the filesystem data being initially mapped for read-only access; and

a processor configured to remap the filesystem data for write access by modifying the read/write flag of the page table entries; to perform a write operation on the filesystem data during write access, and to remap the filesystem data back for read-only access by modifying the read/write flag of the page table entries.

2.   The computing system of claim 1, wherein the processor is to mount the filesystem data in the memory with a protection scheme.

3.   The computing system of claim 1, wherein the processor is to modify page table entries to protect the filesystem data.

4.   The computing system of claim 3, wherein the processor is to modify a read/write flag in at least one page table entry to protect the filesystem data.

5.   The computing system of claim 1, wherein the filesystem data is Linux filesystem data.

6.   A computing system comprising:

at least one random access memory (RAM); and

a filesystem mounted in the RAM to manage filesystem data, the filesystem protecting the filesystem data from errant writes by modifying at least one page table entry associated with the filesystem data without using a disk cache.

7.   The computing system of claim 6, wherein filesystem includes a super block section, inode table section, block in-use bitmap section, and data blocks section.

8.   The computing system of claim 6, wherein the each page table entry includes a read/write flag.

9.   The computing system of claim 6, wherein the filesystem modifies the read/write flag to write-enable mode during a write operation on the filesystem data.

10.   The computing system of claim 9, wherein the filesystem modifies the read/write flat to read-enable after the write operation on the filesystem data.

11.   A computer-implemented method comprising:

mounting a protected filesystem to manage filesystem data in a random access memory (RAM);

calling a protection function when accessing the filesystem data by modifying page table entries to the filesystem data.

12.   The method of claim 11, wherein the filesystem data is initially mapped for read-only access.

13.   The method of claim 12, wherein calling the protection function comprises:

locating page table entries for the protected filesystem;

setting a read/write flag for the located page table entries to write-enable mode;

perform a write operation; and

setting the read/write flay for the located page table entries to read-only mode.

14. A method for protect filesystem data in a protected random access memory (RAM) filesystem, the RAM having RAM pages associated with the filesystem data, the method comprising:

disabling context switching and interrupts when accessing the protected RAM filesystem;

remapping the RAM pages of the protected RAM filesystem for write-enable mode;

performing a write operation on the filesystem data;

remapping the RAM pages of the protected RAM filesystem for read-only mode; and

enabling context switching and interrupts after accessing the protected RAM filesystem.

15. The method of claim 14, wherein remapping the RAM pages for write-enable mode includes:

modifying a read/write flag in the RAM pages for the write-enable mode.

16. The method of claim 15, wherein remapping the RAM pages for read-only mode includes:

modifying a read/write flag in the RAM pages for the read-only mode.

17. The method of claim 15, wherein the read/write flay in the RAM pages is initially set for read-only mode.

18. A computing system comprising:

at least one random access memory (RAM), the RAM having a protected RAM filesystem to manage filesystem data, the filesystem data having RAM pages associated with the filesystem data; and

a central processing unit to disable context switching and interrupts when accessing the protected RAM filesystem, to remap the RAM pages of the protected RAM filesystem for write-enable mode, to perform a write operation on the filesystem data, and to remap the RAM pages of the protected RAM filesystem for read-only mode; and to enable context switching and interrupts after accessing the protected RAM filesystem.

19. The computing system of claim 18, wherein the central processing unit modifies a read/write flag in the RAM pages for the write-enable mode.

20. The computing system of claim 19, wherein the central processing unit modifies a read/write flag in the RAM pages for the read-only mode.

21. The computing system of claim 19, wherein the read/write flag in the RAM pages is initially set for read-only mode.